PCOG Meeting 2016 in Belval

Christian Franck

University of Luxembourg

December 5th, 2016

Outline

- Introduction
- Error-Correcting Codes
- Untraceable Communication

Thank you for invitation!

Communication And Information Theory (CAIN) research group

Prof. Uli SORGER

Dr. Christian FRANCK

Andrea CAPPONI

What we do...

Transmission of data from a sender to a receiver over a noisy communication channel.

Signals

- Modulation/Demodulation,
- Synchronization ...

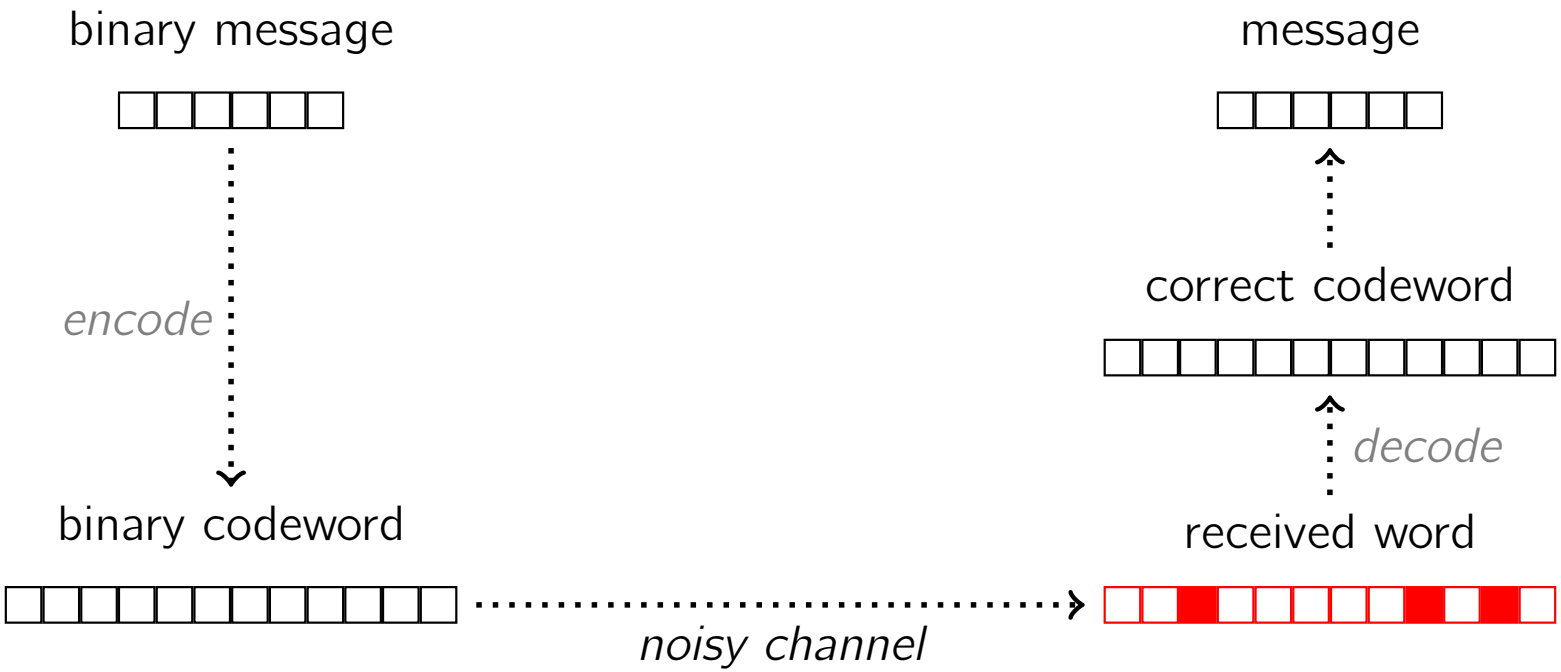
Information Theory

- Source Coding (Compression)
- Channel Coding (Error Correction)

Outline

- Introduction
- Error-Correcting Codes
- Untraceable Communication

My 1st Topic: Error-Correction Codes

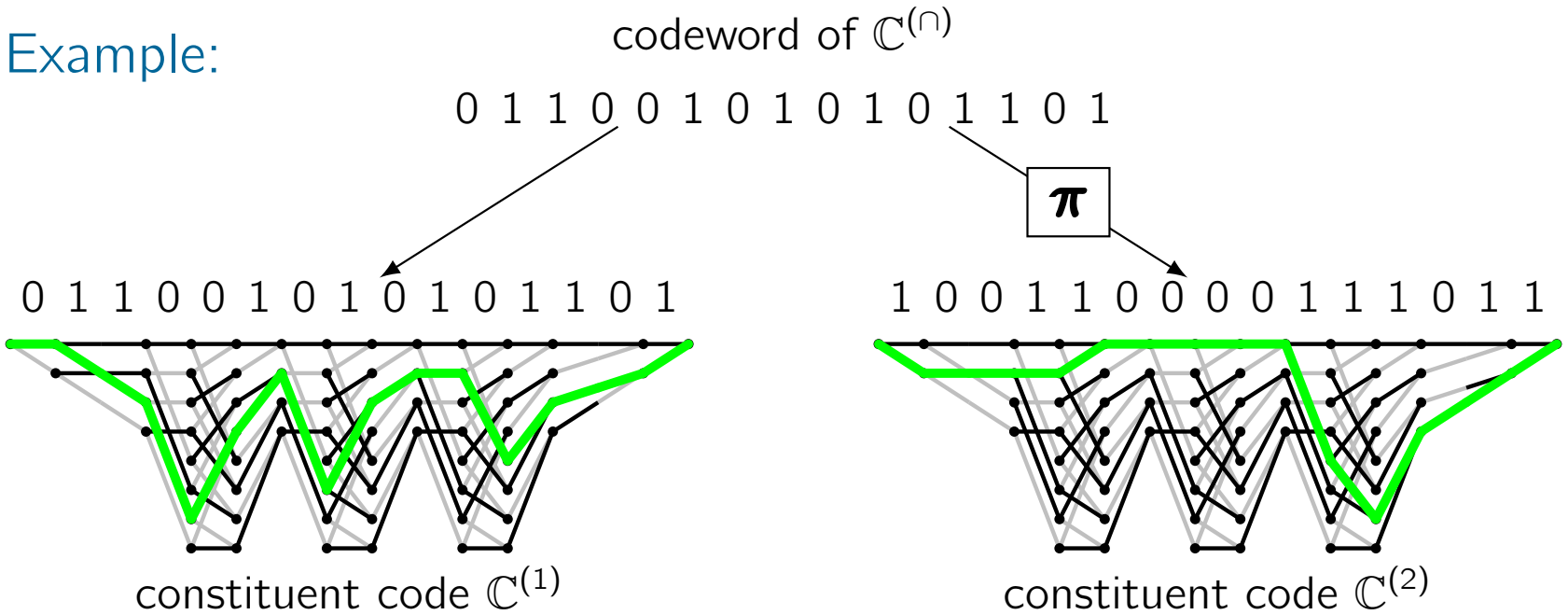


Intersection Codes

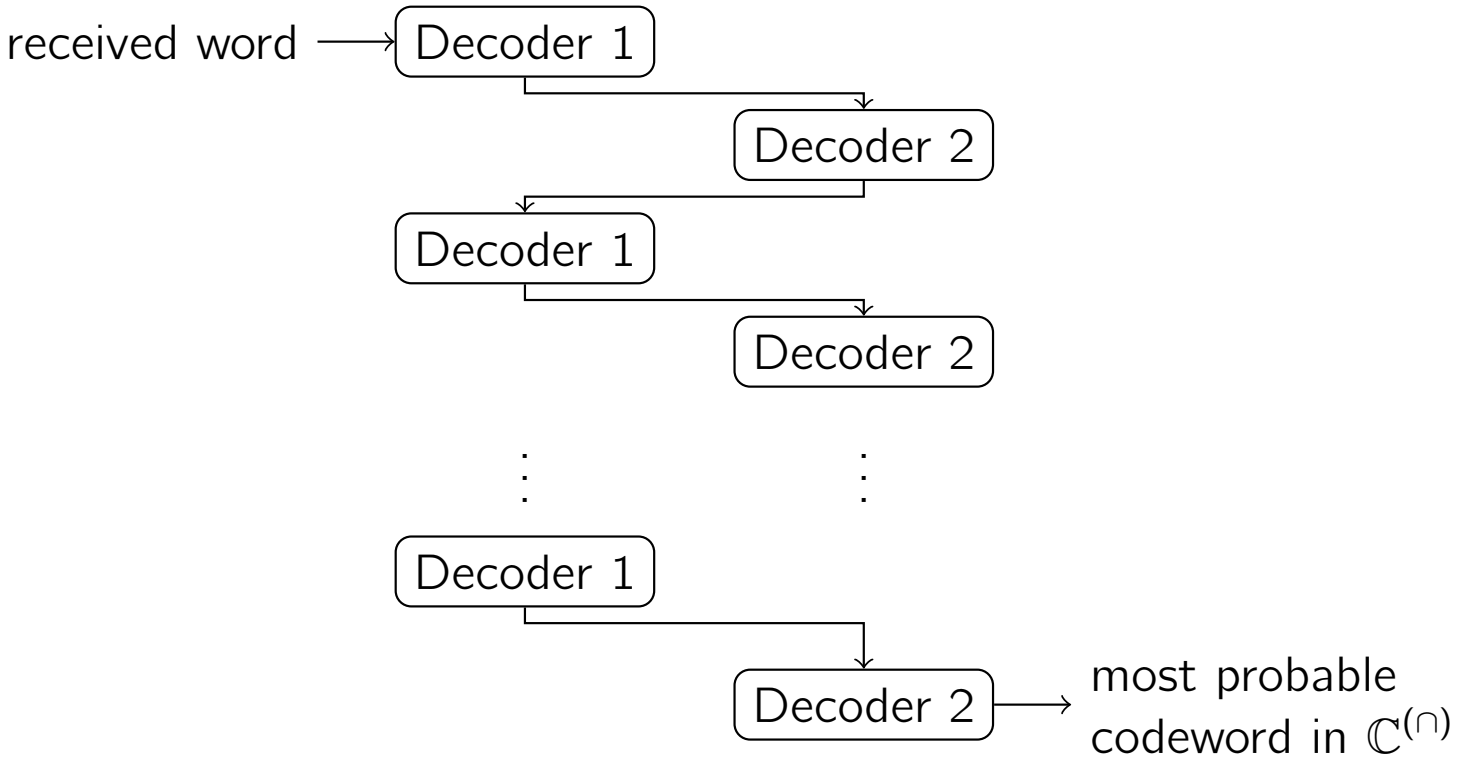
An intersection code $\mathbb{C}^{(\cap)}$ is defined by two constituent codes $\mathbb{C}^{(1)}, \mathbb{C}^{(2)}$ with low trellis complexity, and a permutation $\boldsymbol{\pi}$, with

$$\mathbb{C}^{(\cap)} := \{\mathbf{c} : \mathbf{c} \in \mathbb{C}^{(1)} \text{ and } \mathbf{c}\boldsymbol{\pi} \in \mathbb{C}^{(2)}\}.$$

Example:



Belief Propagation



Problem:

- Only works for some codes.

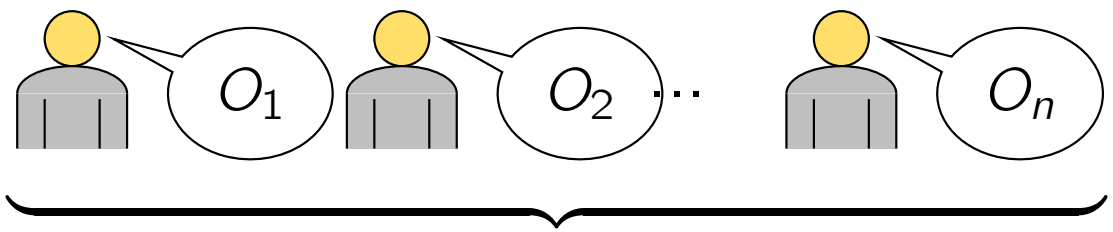
Research:

- Better understanding and improvement of this process.

Outline

- Introduction
- Error-Correcting Codes
- Untraceable Communication

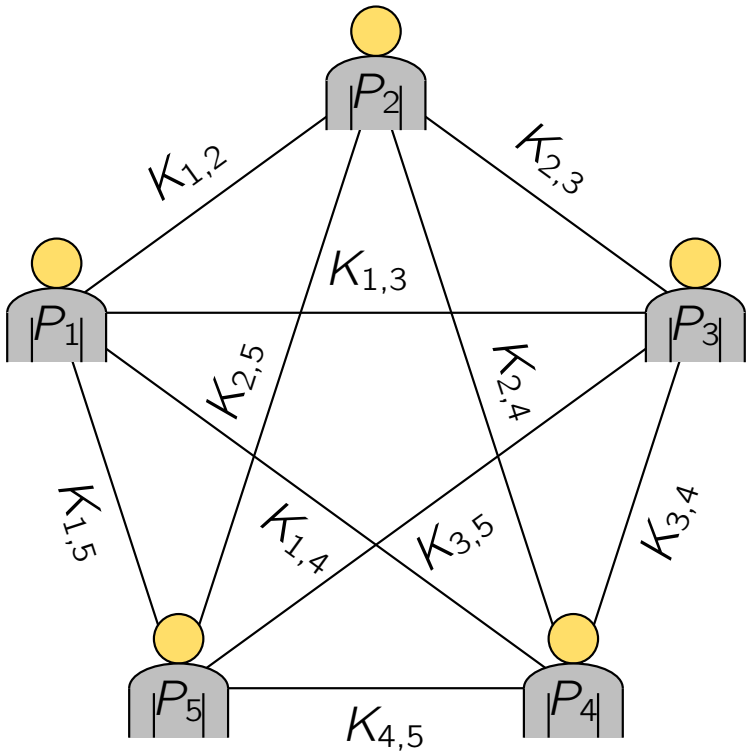
My 2nd Topic: Dining Cryptographers

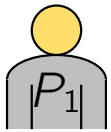


$$M = O_1 \cdot O_2 \cdot \ldots \cdot O_n$$

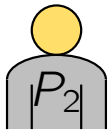
Sender and recipient of message M remain unknown.

Keygraph and Generation of Ciphertexts $O^{(i)}$



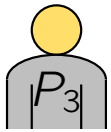


$$O_1 = K_{1,2} \cdot K_{1,3} \cdot K_{1,4} \cdot K_{1,5}$$

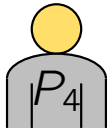


(sender)

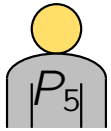
$$O_2 = K_{1,2}^{-1} \cdot K_{2,3} \cdot K_{2,4} \cdot K_{2,5} \cdot M$$



$$O_3 = K_{1,3}^{-1} \cdot K_{2,3}^{-1} \cdot K_{3,4} \cdot K_{3,5}$$

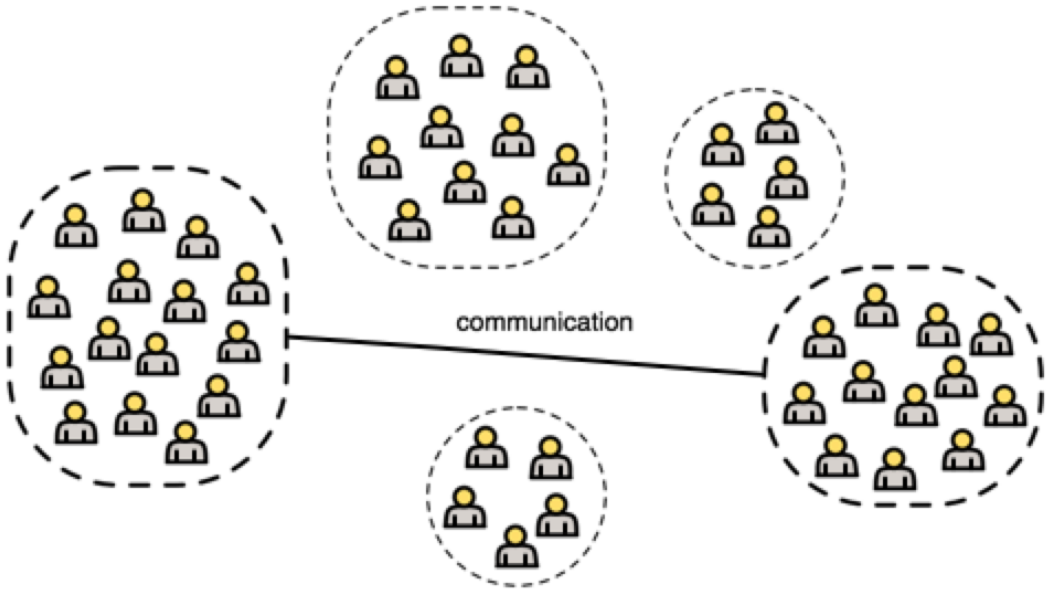


$$O_4 = K_{1,4}^{-1} \cdot K_{2,4}^{-1} \cdot K_{3,4}^{-1} \cdot K_{4,5}$$



$$O_5 = K_{1,5}^{-1} \cdot K_{2,5}^{-1} \cdot K_{3,5}^{-1} \cdot K_{4,5}^{-1}$$

Future: P2P Untraceable Communication Systems



State of the art:

- Many problems (collisions and disruptions) have been solved.

Research:

- Realization of a novel P2P communication systems.

Thank you for your attention!